情報保護學會論文誌
第13券 第5號, 2003. 10

변형된 S박스를 이용한 스트림 암호 알고리즘

박 미 옥*, 최 연 희*, 전 문 석*

Stream Cipher Algorithm using the Modified S-box

Mi-og Park*, Yeon-hee Choi*, Moon-seog Jun*

요 약

무선통신의 발달로 인해 사람들은 언제, 어디서나 서로 통화할 수 있는 시대에 살고 있다. 하지만, 이동통신의 개방성은 심각한 보안위협에 노출되며, 안전한 통신채널을 제공하기 위해 이동통신망에서 보안은 필수적이다. 이동통신망의 보안을 위해서 사용하는 가장 일반적인 방법중의 하나는 스트림 암호이다. 일반적으로, 이 스트림 암호는 LFSR (Linear Feedback Shift Reigster)을 주로 사용하여 구현된다.

본 고에서는 이동통신망의 스트림 암호의 비도를 향상시키기 위해서 블록 암호알고리즘에서 주로 사용하는 S박스의 변형된 메커니즘을 제안하며, 이 메커니즘은 랜덤성을 고려한 3개의 변형된 S박스 메커니즘이다. 일반적으로, S박스는 비선형 특성을 가진 함수로서 임의 데이터를 공격에 더 강하도록 만들어준다. 제안된 알고리즘의 랜덤성 테스트는 Ent 의사난수 테스트 프로그램을 사용하고, 실험결과 각각의 테스트에서 기존의 스트림 알고리즘보다 더 좋은 랜덤성과 serial correlation coefficient를 가진다는 것을 증명한다.

ABSTRACT

Nowadays, people can communicate with each other on any time at any place by develpoment of wireless communications. But, the openness of mobile communications poses serious security threats and the security is necessary on mobile communications to support the secure communication channel. The most commonly method is stream cipher for mobile communications. Generally, this stream cipher is implemented by LFSR(Linear Feedback Shift Register).

On this paper proposes the modified mechanism of the S box is usually used in block cipher to advance security og the stream cipher and this mechanism is the modified three one in consideration og the randomness. Generally, S box that is function with nonlinear property makes data more strong by attack. The randomness test of the proposed algorithm is used Ent Pseudorandom Number Sequence Test Program and by the test result it proves that it has better randomness and serial correlation value than the based stream cipher on respective test.

keyword : *PS-box, random number, stream cipher, mobile security*

Ⅰ. 서 론

이동통신기술의 지속적인 발달로 인하여 사용자들은 언제, 어디서나 원하는 사용자와 통화를 할 수 있을 뿐 아니라 이동단말기를 이용하여 다양한 서비스를 제공받을 수 있다. 하지만, 이동통신의 개방성은 날로 급증하는 무선해킹과 같은 심각한 보안상의 문제점을 드러내고 있다.[1] 이러한 무선상의 보안문제를 해결하기 위한 방법은 데이터를 암호화하는 것이다. 암호알고리즘은 비밀키 알고리즘과 공개키 알고

* 숭실대학교 컴퓨터학과(mopark@kingdom.ssu.ac.kr, nemesis22@hananet.net, mjun@computing.ssu.ac.kr)

리즘으로 구분된다. 공개키 알고리즘은 서로 다른 비밀키와 공개키를 이용해 키 전송이 필요하지 않는 암호방식으로 RSA(Rivest Shamir Adlman), ECC(Elliptic Curve Cryptosystem) 방식 등이 있다. 비밀키 암호방식은 암호화키와 복호화키가 동일한 암호 방식으로 블록 암호(block cipher)와 스트림 암호(stream cipher)로 구분된다. 스트림 암호는 비트열로 입력되는 데이터를 비트단위로 암호화하는 기법이고 블록 암호는 비트열로 입력되는 데이터를 일정한 길이의 비트열로 잘라서 암호화하는 기법이다.[2] 본 고에서 제안하는 알고리즘은 스트림 암호로서 스트림 암호는 채널확산이 없고 비도 수준 요소가 몇 가지 측면에서 수학적으로 보장이 되면 고속처리가 가능한 장점이 있다. 그래서, 스트림 암호는 통신 등에서 사용하는 기술의 발전과 함께 유럽 등지에서 많이 사용되어 왔으며 현대에도 기밀성을 보장하기 위한 용도로 많이 사용된다.[3,4]

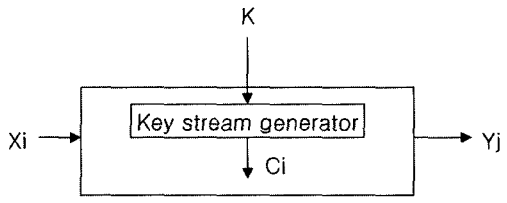
본 고에서는 무선상의 보안을 위해 사용하는 스트림 암호알고리즘의 비도를 높이기 위한 메커니즘으로서 블록 암호알고리즘에서 주로 사용하는 비선형성 S박스를 변형한 메커니즘을 제안한다. 제안한 메커니즘은 스트림 암호알고리즘의 랜덤성을 고려하여 크게 세 가지 방식의 메커니즘을 제안하고, 이에 대한 실험은 기존의 스트림 암호알고리즘과의 비교를 통해 랜덤성(randomness)의 향상을 증명한다.

Ⅱ. 스트림 암호 시스템

본 절에서는 스트림 암호시스템의 일반적인 개념과 동작원리에 대해 설명한다. 스트림 암호시스템은 주로 1970년대 초반부터 유럽에서 연구발전 되어 온 암호시스템으로서 LFSR(Linear Feedback Shift Register)을 이용한 이진수열 발생기이다. 스트림 암호시스템은 최대 주기를 보장하는 LFSR을 비선형으로 결합한 비선형 이진수열 발생기를 근간으로 하는 암호시스템으로 평문을 이진수열로 부호화하여 이진수열 발생기에서 발생된 이진수열과 비트별로 XOR하여 이진수열로 된 암호문을 발생한다. 스트림 암호시스템의 동작을 수식으로 나타내면 다음과 같다.

$$C_i = M_i \oplus K_i \quad \text{for} \quad i=1,2,3... \qquad (1)$$

여기서, C_i는 암호문의 비트열, M_i는 평문문자의 비트열, K_i는 키 수열, ⊕는 XOR 연산자를 나타낸다.



〔그림 1〕 일반적인 스트림 암호시스템

스트림 암호는 동기방식에 따라 자체 동기식(self-synchronization) 스트림 암호와 동기식 스트림 암호로 구분된다. 자체 동기식 암호는 암호문을 입력에 피드백시킴으로서 스트림 동기 이탈시 수신단에서 자체적으로 동기를 복구시킬 수 있는 반면, 채널에서 단 한 비트의 오류가 발생하여도 이동 레지스터 단수 크기의 비트 오류가 확산되므로 채널 오류 대책이 마련된 통신망에서 적용된다. 자체 동기식 스트림 암호에는 Vigenere 암호, 이동 레지스터 방안, 블록 암호화 CFB(Cipher Feedback)모드 등이 있다. 동기식 스트림 암호방식은 스트림 동기 이탈시 자체 복구가 불가능하므로 통신을 중단하고 재동기를 확립해야 하며, 키 수열 발생기, Vernam 암호, 블록 암호의 계수기 등이 있다. 이 방식은 비트 삽입이나 소실과 같은 송수신간의 클럭슬립(clock slip) 발생시 동기가 이탈되는 문제를 보완하여야 하지만 비트 오류의 확산이 없으므로 일반적으로 많이 사용된다.[4]

Ⅲ. 변형된 S박스를 이용한 스트림 암호 알고리즘

본 논문에서는 이동통신상의 무선 채널구간에서 전송되는 데이터를 보다 안전하게 암호화하기 위한 방법으로서 변형된 S(Substitution) 박스의 사용을 제안한다. 일반적으로, S박스는 블록 암호방식에서 주로 사용되는 함수로서, 연산의 효율성 요구조건과 비선형성을 높이기 위해 사용한다. 이 S박스는 비선형 함수를 암호 분석적인 측면에서 안전한 함수를 사용하여 함수의 입출력을 사전에 계산한 테이블 형태로 구성된다.[5] 블록 암호방식에서 주로 사용하는 S박스를 본 고에서 사용할 수 있는 근거는 앞에서 언급한 연산의 효율성과 일반적으로 S박스를 사용하는 이유 중의 하나인 더 안전한 암호학적 강도를 제공한다는 것이다. 이러한 S박스의 일반적인 사용 목적은 본 고에서 제안하고자하는 무선상의 데이터에 더 높은 비도를 제공하기 위한 변형된 S박스의 사용목적과

부합하여 스트림 암호에 S박스를 사용할 수 있는 근거를 제시한다.

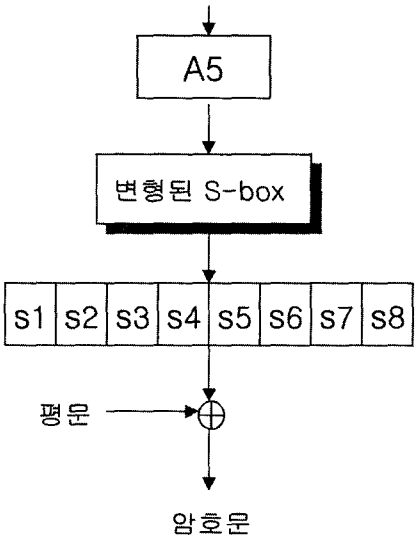
3.1 개념과 구조

본 절에서는 스트림 암호알고리즘의 비도를 높이기 위한 변형된 S박스의 개념과 동작절차를 설명한다. 본 고에서 제안한 변형된 S박스란 기존의 S박스 자체의 내용은 그대로 두고, S박스를 사용할 때 S박스의 입력과정에서 그에 대한 사용순서를 순차적으로 사용하지 않고 랜덤하게 사용하기 위한 방법 하나와 S 박스의 행·열을 결정하기 위한 두 가지 방법을 의미한다. S박스의 사용순서를 비순차적으로 사용하기 위한 방법을 이 후부터는 S박스 결정 메커니즘이라 칭하고, S박스의 행과 열을 결정하는 방법은 S박스 행·열 메커니즘이라고 칭하기로 한다. S박스 결정 메커니즘이란 8개의 S박스가 있고 각 S박스는 나열되어 있는 순서에 따라 번호가 1, 2, 3, ... 으로 되어 있다고 가정할 때, S박스 사용순서를 나열되어 있는 순서인 1, 2, 3, ...의 순서대로 사용하지 않고 3, 1, 7, 6,...의 순서처럼 랜덤하게 사용할 수 있는 방법을 의미한다. S박스 행·열 메커니즘이란 다음 [표 1]에서 보는 바와 같이 S박스안의 어떤 값을 출력하기 위해서 행과 열을 결정하는 방법을 말한다. 본 고에서는 제안한 스트림 암호알고리즘에 더 적합한 S박스 결정 메커니즘과 행열 메커니즘을 제시하여 전체적인 스트림 암호알고리즘의 비도를 높이고자한다.

본 고에서 사용한 S박스는 안전도가 입증된 DES (Data Encryption Standard)의 S박스[6]를 사용하여 변형된 S박스를 제안하고, 비교하기 위한 기존의 스트림 암호알고리즘으로는 A5를 사용한다. A5는 유럽에서 주로 사용하는 이동통신상의 암호알고리즘으로서, 비밀키와 프레임 번호를 입력으로 사용한다. A5는 23단, 22단, 19단으로 구성된 3개의 LFSR을 동작시켜 키 수열을 생성하고,[7,8] 생성된 키 수열은 평문과

〔표 1〕 기존의 S-box 일부

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



〔그림 2〕 제안 알고리즘의 동작절차

함께 XOR을 수행한다.

제안한 모델의 동작원리는 기존 알고리즘이 평문과 XOR을 수행하기 전 단계에서 변형된 S 박스 단계를 통과하도록 하는 것이다. 변형된 S 박스의 통과 과정은 스트림 암호에 비도를 높이기 위한 목적으로 사용되었으며, 이에 대한 개략도는 [그림 2]와 같다.

제안한 모델의 동작절차는 다음과 같다.

[1단계] A5의 입력 : 비밀키에 해당하는 키와 프레임 번호를 입력으로 받는다.
[2단계] A5 알고리즘을 동작한다.
[3단계] A5의 출력 : 키 수열을 생성한다.
[4단계] 변형된 S박스의 입력 : [3단계]에서 출력된 키 수열을 변형된 S박스 메커니즘에 따라 S박스의 입력으로 사용한다.
[5단계] 변형된 S박스를 수행한다.
[6단계] 변형된 S박스의 출력 : [5단계]에서 출력된 결과와 평문에 대해 XOR을 수행한다.

3.2 변형된 S 박스 메커니즘

본 절에서는 변형된 S박스에서 사용하는 S박스 결정 메커니즘과 두 개의 S박스 행·열 메커니즘에 대해 설명한다.

본 고에서 사용하는 S박스 결정 메커니즘은 스트림 암호방식에서 사용된다는 점을 고려하여 간단하

〔표 2〕 S-box 결정 메커니즘

```
Variable + = Value;
S_index = Variable % 사용하는 S박스의 갯수
```

게 랜덤성을 지원할 수 있는 방법을 사용했고, 그에 대한 방법은 [표 2]와 같다. [표 2]에 나타낸 Value는 임의의 랜덤값을 나타내는 변수를 의미하고, Variable은 Value값을 저장할 수 있는 변수를 의미한다. 여기서, Value 변수는 그 값을 변경함으로써 S박스 사용 순서에 랜덤성을 제공하는 역할을 수행한다. S_index는 Variable을 시스템에서 사용하는 S박스의 갯수로 나눈 나머지를 저장하여 그 나머지 값에 따라서 사용하고자 하는 S박스로 분기하게 된다. 예를 들어, 나머지 값이 3이면 사용하는 S박스 중 3번째의 S박스로 분기하게 된다.

이와 같은 간단한 개념에 의해 S박스의 사용순서를 임의적으로 변경해주는 것은 사용순서가 일정할 때 보다 공격에 더 강해짐으로써 알고리즘의 비도를 향상시킬 수 있다.

제안한 모델의 변형된 S박스 통과과정은 S박스의 입력과 출력을 고려해야한다. 사용하는 S박스는 DES의 S박스이기 때문에 DES의 S박스 입력비트인 6비트를 변형된 S박스 단계의 입력에서도 6비트로하여 변형된 S박스를 통과하도록 하고 이를 통과한 출력은 평문과 XOR를 수행한 후 전송된다. 변형된 S박스의 통과과정은 다음과 같이 표현할 수 있다.

$$Out_i = S_i[\ Out_{A5,}\ ] \qquad (2)$$

여기서, $Out_{A5,}$는 변형된 S박스를 통과하기 전의 단계로서 A5를 통과한 후의 출력을 의미하고 동작절차의 3단계에 해당한다. $S_i[]$는 제안 알고리즘에서 사용하는 변형된 S박스를 나타내며 동작절차의 4단계에 속하는 과정이다. Out_i는 5단계의 출력으로서 변형된 S박스의 메커니즘을 통과하고 난 후의 출력을 의미한다. i는 일반적인 의미로서 순서 i번째를 의미한다.

다음은 S박스 행·열 메커니즘을 설명한다. DES의 S박스 행·열 결정방법은 $S(\ b_0\ b_1\ b_2\ b_3\ b_4\ b_5)$의 6개 비트 중 첫번째 비트 b_0와 여섯번째 비트 b_5로 행을 결정하고, 나머지 두번째부터 네번째 비트 $b_1\ b_2\ b_3\ b_4$의 4개 비트를 가지고 열을 결정한다. 본 고에서 사용하는 첫번째 행·열 메커니즘은 DES의 S 박스 원리에 따라 2개 비트로 행을 결정하고 4개의 비트로 열을 결정하지만, 행을 결정하는 비트를 첫번째 비트 b_0와 두번째 비트 b_1으로 하고, 3, 4, 5, 6번째 비트 $b_2\ b_3\ b_4\ b_5$가 열을 결정하는 방법을 사용한다. 이러한 방법을 사용한 이유는 기존의 블록암호에서의 S박스는 알고리즘의 내부에서 평문을 충분히 암호화시키기 위해서 블록단위의 평문들과 함께 혼동과 확산을 위해 비슷한 위치의 데이터들이 의존도가 낮은 다른 위치나 다른 데이터로 치환, 대치되기 위해 사용되지만, 본 알고리즘에서 사용하는 변형된 S박스는 그 적용부분이 기존 알고리즘의 내부가 아닌 평문과 XOR을 수행하기 전의 바로 전 단계에 적용되어 이 단계에서의 출력 값은 어느 정도의 랜덤특성을 가지도록 암호화된 결과값이고, 이러한 랜덤 특성을 가진 결과값들이 행열을 결정하기 위해 사용되기 때문에 DES의 행열 결정방법에 의해 반드시 첫번째와 여섯번째 비트가 아니더라도 행과 열을 결정할 수 있기 때문이다. 그리고, DES 내부에서 사용되는 S박스는 블록 암호방식이기 때문에 한꺼번에 블록단위로 처리하기위해 첫번째와 여섯번째 비트를 동시에 처리하지만, 제안모델에서 사용하는 알고리즘은 스트림 암호알고리즘으로서 비트단위로 순차적으로 처리되기 때문에 행을 결정할 때 처음에 생성된 두비트를 순차적으로 사용하여 행을 결정하는 것이 더 타당하다고 본다. 또한, 기존의 행열방법처럼 행을 위한 첫번째 비트가 생성되고 그 다음에서 열을 위한 4개의 비트가 생성되고, 또 다시 행을 위한 여섯 번째 비트가 생성되는 것보다 처음 두비트로 행을 결정하고 나머지 비트로 열을 결정하는 방법이 개념상으로도 간단하여 스트림 암호에 더 적합하다고 판단되기 때문이다. 첫번째 행·열 메커니즘은 다음 [표 3]과 같다.

첫 번째 행·열 메커니즘을 사용한 스트림 암호알고리즘과 DES 행열방법에 의한 알고리즘의 랜덤성 테스트를 4장에서 비교·실험하였고, 실험 결과 첫번째 행·열 메커니즘이 DES 행열방법보다 더 좋은 랜덤성을 나타내어 본 고에서 제시하는 첫 번째 행·열 메커니즘의 타당성을 증명한다. 또한, 기존의 스트림 알고리즘과의 실험을 통해 더 좋은 랜덤성과 상관 특성을 가진다는 것을 증명하여 제안 모델의 비도가 향상됨을 보인다.

다음은 본 고에서 제시하는 두 번째 행·열 메커니즘이다. 두 번째 행·열 메커니즘은 앞에서 사용한 행·열 메커니즘에서 열을 결정하는 부분에 4개 비트가 사용됨에 따라 열에 치우친 계산량을 줄이기 위해 행과 열을 결정할 때 각각 3개의 비트를 사용

〔표 4〕 S박스 행·열 메커니즘(2)

```
S_row = gb[0]*2 + gb[1];
S_col = gb[2]*8 + gb[3]*4 + gb[4]*2 + gb[5];
S_out = S_box[S_index][S_row*S+col];
```

〔표 5〕 수정된 8X8 행열 S-box

	0	1	2	3	4	5	6	7
0	14	4	13	1	2	15	11	8
1	3	10	6	12	5	9	0	7
2	0	15	7	4	14	2	13	1
3	10	6	12	11	9	5	3	8
4	4	1	14	8	13	6	2	11
5	15	12	9	7	3	10	5	0
6	15	12	8	2	4	9	1	7
7	5	11	3	14	10	0	6	13

하는 방법을 제시한다. [표 4]에 나타낸 두 번째 행·열 메커니즘은 행을 결정하기 위해 처음에 생성된 3개의 비트를 사용하고, 다음에 생성된 3개의 비트를 열을 결정하기 위해 사용한다.

각각 3비트를 사용하는 행·열 메커니즘에서는 기존의 [표 1]에 나타낸 4X16 행열 S박스 형태를 [표 5]와 같은 8X8 행열 형태로 변경하여 사용한다. 그래서, 수정된 8X8 행열 S박스형태에서도 기존의 DES S박스 내용을 그대로 사용가능하도록 지원한다. [표 5]에서 음영이 들어간 부분은 음영이 없는 바로 앞 행의 마지막 부분으로 이동시키면 기존의 S박스와 동일한 형태가 된다. 예를 들어, [표 5]의 0행에 나타난 데이터 [14,4,13,1,2,15,11,8]의 끝 부분에 1행의 데이터 [3,10,6,12,5,9,0,7]을 연이어 쓰게 되면 [표 1]에 나타낸 DES S박스의 0행에 해당하는 원래 데이터 [14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7]가 다시 만들어진다. 그래서, 두번째 행열 메커니즘은 기존의 S박스의 한 행을 절반으로 나눈 데이터들 중 첫번째 데이터 값이 두번째 데이터 값이 나오는 행의 바로 행에 오도록 하는 나열방식을 사용한다.

두번째 행·열 메커니즘의 8X8 행열 S박스가 첫번째 행·열 메커니즘의 4X16 행열 형태와 다르게 구성할 경우 S박스 자체의 변화를 조사하기 위해서 하나의 S박스를 임의로 선택해 4장에서 테스트하였다. 또한, 수정된 S박스형태를 8개의 모든 S박스에 적용하여 첫번째 행·열 메커니즘과 비교·실험하고, 기존의 DES 행열방식과도 비교·실험한다. 실험결과, 각각의 실험횟수에서 첫번째 제안모델보다 더 좋은 랜덤 확률을 보여 결과적으로, 첫번째와 두번째 행·열 메커니즘을 사용한 제안모델은 기존의 스트림 모델보다 더 안전하다고 할 수 있다.

이러한 방법으로 4단계의 S박스 과정을 통과한 출력 비트는 평문과 XOR을 수행하고, 제안 알고리즘의 최종적인 출력은 다음과 같이 표현할 수 있다.

$$C_{i=} S_i[\ Out_{A5,}] \oplus P_i \qquad (3)$$

여기서, C_i는 ciphertext인 암호문, $S_i[Out_{A5,}]$는 앞의 식 2와 동일한 의미로서 S박스를 통과한 4단계의 출력을 의미한다. P_i는 plaintext로서 C_i와 XOR를 수행할 평문을 나타낸다. XOR 연산은 ⊕로 표기하고, i는 i번째의 순서를 의미한다.

Ⅳ. 실험 결과 및 분석

본 절에서는 먼저 기존의 스트림 암호알고리즘과 제안한 모델을 비교·실험하고, 다음으로 제안한 모델에서 사용하는 몇 가지 메커니즘들을 비교·실험하여 그에 대한 효율성을 검증한다. 검증을 위한 실험환경은 UltraSPAC-II 400MHz(두개)의 CPU와 2048M의 메모리, 디스크는 8G(7개)인 Sun Enterprise 3500에서 실험하였고, 사용한 언어는 C언어이다. 각 출력 수열의 랜덤성 여부를 테스트하기 위해 Ent(Pseudorandom Number Sequence Test Program)프로그램을 사용하였다. Ent 프로그램은 의사난수 시퀀스의 랜덤성 테스트를 위해 John Walker에의해 작성된 프로그램으로서 entropy, optimum compression, chi square distribution for samples, arithmetic means for data bytes, monte carlo value for Pi, serial correlation coefficient와 같은 항목을 측정할 수 있다.[9] Ent의 입력으로 사용하는 총 비트는 임의의 횟수로 나누어 그 횟수만큼 반복 실험하였다. 예를 들어, 실험에 총 100비트를 사용하고 실험횟수가 10번이라고 한다면, 총 100비트를 10으로 나눈 결과값이 10이 되기 때문에 1번 실험에 10비트를 사용하여 랜덤성을 테스트하고, 2번째 실험에서는 1번째 실험에 사용된 10비트에 그 다음의 새로운 10비트를 합친 20비트에 대해 랜덤성을 실험한다. 그 다음 3번째 실험은 2번째 실험에 사용된 20비트에 다시 새로운 10비트를 합친 30비트에 대한 테스트를 하는 방식으로 실험하였다. 이런 방법은 각 모델의 최종값만 비교하는 것이 아니라 각 반복실험마다 상대적으로 얼마나 좋은 랜덤성과 상관특성을 나타내는지를 조사하기 위해서이다.

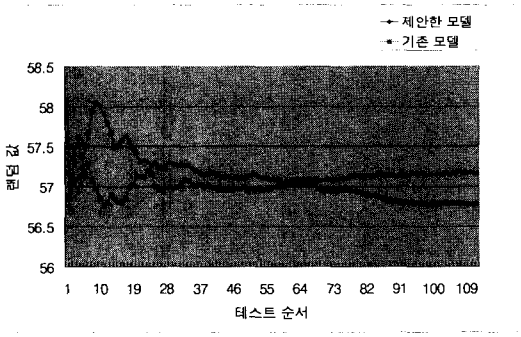
4.1 기존모델과 제안모델에 관한 고찰

본 절에서는 기존의 알고리즘과 본 고에서 제안한 첫 번째 행·열 메커니즘을 사용한 모델을 비교실험한다. 테스트를 위해 사용한 비트는 약 30500 비트이며, 앞에서 예를 든 실험방법에 따라서 127번의 횟수로 나누어 랜덤검정을 수행하였다.

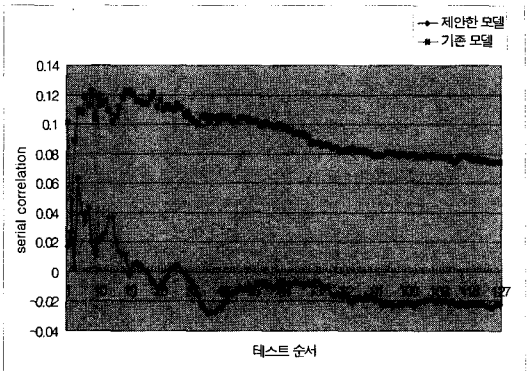
[그림 3]는 랜덤 검정을 수행한 결과를 나타낸 것으로, 그림에서 보는 것처럼 사용한 비트가 증가함에 따라 변동이 심했던 처음의 랜덤 값이 제안한 모델에서는 2번 56.대의 값을 나타

내는 것을 제외하고는 모두 57.대와 58.대의 arithmetic mean값을 출력하고, 기존모델에서는 처음 몇 번의 57.대의 값을 제외하고는 비트가 증가할수록 56.대로 값이 감소하는 것을 볼 수 있다. 실험 횟수로 비교할 때는 제안한 모델이 127번 중 124번 더 높은 랜덤 값을 출력하고, 기존모델은 처음 부분의 3번만 더 높은 값을 출력했다. 여기서 arithmetic mean 테스트는 파일 안의 모든 바이트를 합하여 파일 길이로 나눈 결과로서, 약 127.5에 가까울수록 좋은 랜덤성을 의미하기 때문에 제안모델은 기존모델보다 더 좋은 랜덤성을 나타낸다고 말할 수 있다.

Serial correlation는 파일 안의 각 바이트와 이전 바이트와의 의존도를 나타내는 것으로서, 양수나 음수의 값을 가질 수 있으며 0에 가까워야 더 좋은 상관특성을 가진다. [그림 4]에서 보는 것처럼 전반적으로 제안모델이 기존모델보다 0에 훨씬 가까운 값을 나타내는 것을 알 수 있고, 비트가 증가할수록 기존모델은 0.08대의 값에 가까워지고 제안모델은 0.02대의 값에 가까워지는 것을 볼 수 있다. 이것은 제안모델이 기존모델보다 각 바이트와의 의존도가 더 낮기 때문에, 상관 공격에 더 강하여 비도가 향상됨을 나타낸다.



〔그림 3〕 제안한 모델과 기존모델과의 비교(1)

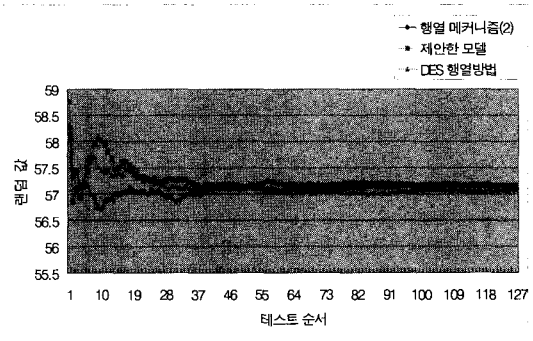


〔그림 4〕 제안한 모델과 기존모델과의 비교(2)

4.2 세 가지 메커니즘에 관한 고찰

그림과 표는 본 절에서는 제안한 첫번째 행·열 메커니즘과 두번째 행·열 메커니즘, 그리고 기존의 DES S박스 행·열 메커니즘에 대한 랜덤성을 테스트하여 DES의 S박스 행·열 메커니즘을 변형하여 사용할 경우 랜덤성에 미치는 영향을 알아본다. 또한, 본 절에서는 임의의 한 S박스를 선택해 첫번째 행·열 메커니즘, 두번째 행·열 메커니즘, DES의 S박스 행·열 메커니즘을 각각 적용하여 테스트 할 경우 기존의 DES의 S박스 자체에 어떠한 변화를 보이는가를 실험한다.

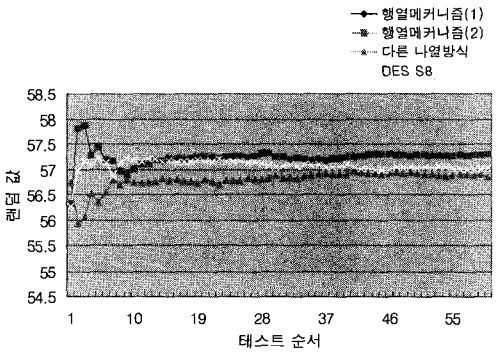
먼저, 두번째 행·열 메커니즘과 [그림 3]와 [그림 4]에서 제안한 모델이라고 표시된 첫번째 행·열 메커니즘, 그리고 기존의 DES S박스 행·열 메커니즘에 대한 랜덤성 결과는 [그림 5]과 같다. 실험에 사용한 비트는 약 30500 비트를 127번 나누어 테스트하였다. 실험 결과 두번째 행·열 메커니즘은 제안한 모델에 비해 127번 중 75번 더 좋은 랜덤 값을 나타냈고, 기존의 DES 행열 방법과의 비교에서는 127번



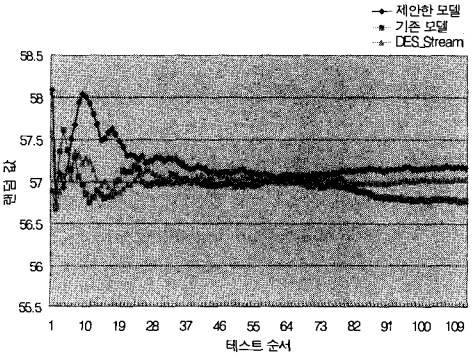
〔그림 5〕 세 개의 행·열 메커니즘 비교

중 87번 더 좋은 랜덤값을 나타냈다. 제안모델과 DES 행열 방법과의 비교는 127번 중 107번 더 좋은 결과를 출력하였다. 비트가 증가할수록 세 방법은 변동이 심하지 않고 일정한 값을 유지하는 것을 볼 수 있으며 제안모델과 두번째 행·열 메커니즘을 사용한 모델이 기존의 DES S 박스 행열 방법을 사용한 모델보다 더 좋은 결과를 나타냄으로써 본 고에서 제시하는 두가지 행·열 메커니즘의 효율성을 증명한다.

다음은 변형된 S박스 결정 메커니즘을 사용하지 않은 첫번째 행·열 메커니즘과 두번째 행·열 메커니즘, 그리고 DES의 행열 메커니즘을 사용하여 임의의 한 S박스를 선택하여 랜덤성을 테스트하였다. 이것은 기존의 DES S박스 형태가 아닌 두번째 행·열 메커니즘을 사용하였을 때 기존의 DES S박스에 대한 변화를 조사하기 위한 것이다. [그림 6]에서 행열 메커니즘(1)과 (2)는 각각 첫번째 행열 메커니즘과 두번째 행열 메커니즘을 의미하고, DES S8로 표시된 부분은 DES의 S박스 행열 메커니즘을 의미하고, 테스트에 사용한 S박스는 여덟번째(S8) 박스를 선택하여 세 개의 방법에서 각각 실험하였다.



[그림 6] S8 박스에 대한 랜덤성 비교



[그림 7] S박스 결정 메커니즘에 대한 비교

[그림 6]에서 보는 것처럼, 하나의 S8 박스에 대한 첫번째 행·열 메커니즘과 두번째 행·열 메커니즘은 동일한 결과값을 출력하였고, DES S박스 행·열 메커니즘을 사용하여 S8 박스를 실험한 결과는 127번의 횟수 중 6번만 제안한 두 가지 방법보다 더 좋은값을 출력하여 결과적으로 임의의 한 S박스를 선택하여 세 가지 방법을 테스트한 결과 제안한 방법이 더 좋은 랜덤특성을 나타내는 것을 알 수 있다. 여기서 한 S박스에 대한 첫번째 행열 메커니즘과 두번째 행열 메커니즘의 출력이 동일하다는 것은 4X16 행열인 S박스를 8X8 행열로 구성하더라도 S박스 자체에 변화가 없음을 나타낸다고 말할 수 있다. 이와 같은 동일한 결과가 나오는 이유는 [표 5]에서 설명한 수정된 8X8 행열이 기존의 4X16 형태인 박스안의 한 행을 두 개로 나누어 나눈 앞 부분의 데이터를 뒷 부분의 데이터 바로 앞의 행에 나열하는 나열방식의 특성 때문인 것으로 보인다. 동일한 결과값이 나열 방식의 특성 때문에 발생하는지를 조사하기 위해 [표 5]의 형태가 아닌 다른 나열방식을 사용한 8X8 형태로 실험해 본 결과 다른 결과 값을 출력함으로써, [표 5]의 나열방식 특성은 S박스 안의 한 행을 구성한 함수자체에 변화를 주지 않는 것으로 증명되었다. 다른 나열 방식을 사용한 결과는 [그림 6]에 다른 나열방식이라는 범례로 표시하였다.

다음은 변형된 S박스 결정메커니즘을 사용한 제안모델과 S박스 결정 메커니즘의 순서를 순차적으로 사용하고, S박스 행열 메커니즘도 DES에서 사용하는 방식대로 0과 5번째 비트로 행을 결정하도록 한 모델인 DES_Stream이라고 칭한 모델과의 비교를 통해 변형된 S박스 결정 메커니즘이 랜덤성에 미치는 결과를 테스트한다. [그림 7]에서 보는 바와 같이 제안모델이 전체적인 부분에서 127번 중 126번 DES_Stream 모델보다 더 좋은 랜덤특성을 나타내는 것을 확인할 수 있다. 결과적으로, 제안모델은 DES의 순차적인 S박스 사용과 첫번째와 여섯번째 비트를 사용하여 행을 결정하는 기존의 DES S박스 행열방식보다 더 좋은 랜덤특성을 제공한다고 말할 수 있다.

4.3 안전성 분석

4.3.1 비선형 함수

먼저 S박스 사용과 비도와의 관계를 설명한다. 제안한 모델에서는 비선형 함수의 특성을 가지는 변형

된 S박스의 사용을 제안하였다. 일반적으로 함수가 선형적이면 결과를 통해 입력을 유추하기가 비교적 쉽다. S박스는 비선형 성질을 갖도록 하여 이러한 선형함수의 단점을 보완하는 역할을 함으로써 블록 암호알고리즘의 비도를 높이는 일반적인 방법으로 사용된다. 또한 lookup table로서 이미 계산이 되어 있는 형태이기 때문에 사용할 때마다 계산을 해야하는 연산의 비효율성을 줄일 수 있다. 이와 같은 특성은 비선형 함수인 S박스를 스트림 암호알고리즘에 적용함으로써 불안전한 기존의 스트림 알고리즘에 비선형 특성을 부여하여 출력에 의한 입력을 유추하기가 더 어렵게 되기 때문에 결과적으로 스트림 암호알고리즘의 비도를 높인다고 말할 수 있다. LFSR을 결합하여 사용하는 스트림 암호알고리즘은 상관공격(correlation attack)이란 강력한 공격방법에 의하여 대부분 약점이 있음이 밝혀졌다.[3,5] 하지만, S박스는 선형공격에 강하도록 입·출력의 상관계수가 작도록 설계되기 때문에 S박스를 적용한 제안모델은 상관공격에 더 강하여 기존의 스트림 암호알고리즘보다 더 높은 비도를 제공한다고 말할 수 있다. 이에 대한 테스트는 4.1절을 통해 검증하였다. 또한, 빠른 계산시간을 필요로 하는 스트림 암호알고리즘의 특성상 사용할 때마다 계산을 해야하는 비선형 함수를 사용하는 것이 아니라 이미 계산이 되어있는 비선형 함수인 S박스를 사용하기 때문에 연산의 효율성을 가진다고 말할 수 있다.

다음은 S박스 결정 메커니즘과 비도와의 관계를 설명한다. [표 2]에서 제시한 S박스 결정 메커니즘은 변수 Value에 임의의 랜덤값을 저장시켜서 S박스 사용순서에 비순차성을 제공한다. 또한, Value 변수는 그 값을 임의적으로 변경시킴으로써 S박스 사용순서가 그 전의 순서와는 다르게 사용될 수 있게 하였다. 이러한 S박스 사용순서를 비주기적으로 변경하는 방법은 사용순서가 일정할 때의 출력값에 비해 일정한 패턴을 찾기가 더 어렵기 때문에 공격에 더 강해짐으로써 더 높은 비도를 제공한다고 할 수 있다.

4.3.2 랜덤성과 상관 특성

스트림 암호에서의 비도 수준은 암호 공격에 강한 키 수열 발생기의 설계에 의해 결정되므로 일반적으로 키 수열의 주기에 대한 최대값의 보장, Golomb의 좋은 랜덤특성, 좋은 상관 면역성을 가질 것, 큰 선형복잡도를 가질 것 등의 요구사항을 만족해야 한다.[10] 본 절에서는 제안한 모델의 비도조건 중 좋은 랜덤특성과 좋은 상관면역성에 대한 조건을 실험 결과를 분석함으로써 제안한 모델의 비도가 증가함을 밝힌다.

좋은 랜덤 특성에 대한 조건은 4.1과 4.2절의 실험에서 arithmetic mean값으로 측정되었다. [그림 4]에서 보는 바와 같이 제안모델은 기존모델보다 더 높은 arithmetic mean값을 출력하기 때문에 앞에서 밝힌 arithmetic mean의 정의에 따라서 더 좋은 랜덤 특성을 나타내어 두번째 비도 조건에 대해 제안모델이 기존모델보다 더 높은 비도를 제공한다고 말할 수 있다.

좋은 상관 면역성을 가져야한다는 조건은 serial correlation값으로 측정되었다. [그림 4]에서 보는 바와 같이, 제안모델은 기존모델에 비해 0에 훨씬 더 가까운 값을 출력함으로써 앞에서 밝힌 serial correlation의 정의에 따라 상관특성이 향상됨을 알 수 있다. 상관특성이 향상되었다는 것은 바이트들의 의존도가 그 만큼 낮기 때문에 상관공격에 의한 입·출력과의 일정한 패턴을 찾기가 더 어렵게 되어 공격에 더 강해진다. 이 테스트는 비도 조건 중 세 번째 조건에 대해 제안모델이 기존모델보다 훨씬 더 좋은 특성을 가진다는 것을 의미한다.

결과적으로, 두 개의 비도 조건에서 제안모델이 기존모델보다 더 좋은 특성을 나타내기 때문에 제안모델이 더 높은 비도를 나타낸다고 말할 수 있다.

V. 결 론

본 고에서는 블록 암호알고리즘에서 주로 사용하는 S박스를 변형한 메커니즘을 스트림 암호알고리즘에 적용하는 방법을 제안하였다. 본 고에서는 변형된 메커니즘을 변형된 S박스로 칭하였고, 변형된 S박스 메커니즘에는 S박스를 사용하는 순서를 비순차적으로 사용할 수 있는 S박스 결정 메커니즘과 S박스의 행과 열을 결정하는 방법으로 두개의 행·열 메커니즘을 제안하였다. 제안한 각각의 메커니즘들은 랜덤성 여부에 대해 기존의 스트림 암호알고리즘인 A5알고리즘과 비교·분석하여, 테스트 결과 제안한 모델의 3가지 메커니즘이 기존의 메커니즘보다 더 좋은 랜덤성과 0에 더 가까운 serial coefficient값을 출력함으로써 제안모델의 효율성을 증명하였다. 본 고는 이동통신 시스템의 암호알고리즘의 개발과 스트림 암호기가 필요한 디지털 서명과 같은 분야에 응용되어질 수 있을 것으로 기대된다. 향후 과제로는 무선채

널상에 보다 타당한 S박스의 선택과 활용에 대한 연구가 필요하리라 보며, 이에 따라 더 높은 비도를 제공할 수 있는 S박스에 대한 연구도 필요하리라 본다.

참 고 문 헌

[1] 양형규, 안영화, "난수와 암호", *통신정보학회논문지* (C), 3(2), pp.115~126, 1992.9.

[2] 진앙규, 임환주, 김창규, 이만영, "다수의 원시다항식을 이용한 비선형 스트림 암호기와 오류제어에 관한 연구", *한국통신학회 추계종합학술발표회 논문집*, pp.219~224, Nov. 1990.

[3] 지성택, 박춘식, "비밀키 암호", *TELECOMMUNICATIONS REVIEW:*, 10(5), pp.877~885, Sep-Oct. 2000.

[4] 박종욱, 황인호, 홍재근, "RMVD를 이용하는 동기식 스트림 암호 데이터 통신시 난수동기 이탈 검출 알고리즘", *정보보호학회논문지*, 10(5), pp. 21~29, 2000.

[5] 김범식, 신인철, "해쉬함수와 스트림 암호기의 개발 및 GSM 보안 시스템에의 적용", *한국정보처리학회논문지*, 7(8), pp.2421~2429, Aug 2000.

[6] Johannes A. Buchmann, "Introduction to Cryptography", *Springer-Verlag*, pp.115~125, 2000.

[7] Alx Biryukov, Adi Shamir, David Wager, "Real Time Cryptanalysis of A5/1 on a PC", *Fast Software Encryption Workshop 2000*, 40, pp. 71-79, April. 2000.

[8] Uyless Black, "MOBILE AND WIRELESS NETWORKS," *Prentice Hall Series in advanced communications technologies*, pp.176~209, 1996.

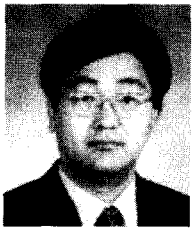
[9] John, W., "ENT A Pseudorandom Number Sequence Test Program," *http://www.fourmilab.ch/random/*

[10] 홍진근, 손해성, 황찬식, 김상훈, 윤기철, "무선채널에서의 암호통신을 위한 통시기 스트림 암호 시스템 구현", *한국통신학회논문지*(C), 24, pp.894~904, 1999.6.

〈著者紹介〉

박 미 옥 (Mi-og Park) 학생회원
1991년 2월 : 조선대학교 전산통계학과 졸업
1993년 2월 : 숭실대학교 컴퓨터학과 석사 졸업
1996년 3월~현재 : 숭실대학교 컴퓨터학과 박사과정
<관심분야> 이동통신 보안, 차세대 이동통신, 정보보안

최 연 희 (Yeon-hee Choi) 학생회원
1991년 2월 : 목포대학교 전산통계학과 졸업
1993년 2월 : 숭실대학교 컴퓨터학과 석사 졸업
1996년 3월~현재 : 숭실대학교 컴퓨터학과 박사과정
<관심분야> 정보보안, 암호학



전 문 석 (Moon-seog Jun) 종신회원
1986년 : University of Maryland 전산과 석사
1989년 : University of Maryland 전산과 박사
1989년 : Morgan State University 전산수학과 조교수
1989년~1991년 : New Mexico State University 부설 Physical Science Lab.책임연구원
1991년~현재 : 숭실대학교 정보과학대학 정교수
<관심분야> 네트워크 보안, 컴퓨터 알고리즘, 병렬처리, VLSI 설계, 암호학